(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2003 (24.04.2003)

PCT

(10) International Publication Number
WO 03/034193 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US02/33072

(22) International Filing Date: 17 October 2002 (17.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/346,802 18 October 2001 (18.10.2001) US
10/081,173 22 February 2002 (22.02.2002) US

(71) Applicant: MACROVISION CORPORATION [US/US]; 2830 De La Cruz Boulevard, Santa Clara, CA 95050 (US).

(72) Inventor: COLLIER, David; 1494 East Hillview Court, Gilroy, CA 95020 (US).

(74) Agent: NGUYEN, Frank; For Macrovision Corporation, 2830 de la Cruz Blvd., Santa Clara CA 95050 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 03/034193 A2

(54) Title: METHOD, APPARATUS AND SYSTEM FOR SECURELY PROVIDING MATERIAL TO A LICENSEE OF THE MATERIAL

(57) Abstract: A method, apparatus and system for securely providing material to a licensee of the material are described. In each, at least one license key is provided, preferably along with a license including usage rights for requested content or material to the licensee. The material requested and licensed by the licensee is provided to the licensee encrypted with at least one content key. To achieve a second-level of security, the at least one content key is provided to the licensee encrypted with the at least one license key so that both the at least one content key and the at least one license key are necessary for the licensee to decrypt and use the encrypted material.

METHOD, APPARATUS AND SYSTEM FOR SECURELY PROVIDING MATERIAL TO A LICENSEE OF THE MATERIAL

FIELD OF THE INVENTION

The present invention generally relates to techniques for preventing unauthorized use of material and in particular, to a method, apparatus and system for securely providing material to a licensee of the material.

BACKGROUND OF THE INVENTION

Providers of material demand compensation for the use of their material or content. Unauthorized use cheats these providers of their due compensation. Therefore, techniques for preventing such unauthorized use have been and continue to be developed. As soon as new techniques are developed and practiced, however, dishonest users seek to circumvent those techniques to avoid paying compensation to the content providers. Consequently, techniques for preventing unauthorized use of material evolve to stay one step ahead.

OBJECTS AND SUMMARY OF THE INVENTION

Accordingly, it is an object of the present invention to provide a method for securely providing material to a licensee of the material.

Another object is to provide an apparatus for securely providing material to a licensee of the material.

Still another object is to provide a system for securely providing material to a licensee of the material.

These and additional objects are accomplished by the various aspects of the present invention that uses at

least a two-key approach for added security. Briefly stated, one aspect is a method for securely providing material to a licensee of the material that includes providing at least one license key to a licensee of material; providing the material encrypted with at least one content key to the licensee; and providing the at least one content key encrypted with the at least one license key to the licensee.

Another aspect is an apparatus for securely providing material to a licensee of the material. The apparatus includes at least one server that is configured to transmit at least one license key to a client device operable by a licensee of material; transmit the material encrypted with at least one content key to the client device; and transmit the at least one content key encrypted with the at least one license key to the client device.

Another aspect is a system for securely providing material to a licensee of the material. The system includes a client device operable by a licensee of material; and at least one server configured to transmit at least one license key, the material encrypted with at least one content key, and the at least one content key encrypted with the at least one license key to the client device.

Still another aspect is a method for securely providing material to a licensee of the material that includes providing a license to use material and a license key corresponding to the license; providing the material encrypted with a content key; and providing the content key encrypted with the license key.

Yet another aspect is a method for securely providing material to a licensee of the material that includes receiving a license to use material and a license key corresponding to the license; receiving the material encrypted with a content key; receiving the content key encrypted with the license key; decrypting the encrypted

content key using the license key; and decrypting the encrypted material using the decrypted content key.

Additional objects, features and advantages of the various aspects of the present invention will become apparent from the following description of its preferred embodiments, which description should be taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a flow diagram of a method implemented, for example, by one or more servers for securely providing material to a licensee of the material, utilizing aspects of the present invention.

FIG. 2 illustrates a flow diagram of a method implemented, for example, by a client for securely providing material to a licensee of the material, utilizing aspects of the present invention.

FIGS. 3~4 illustrate, as examples, block diagrams of three systems for securely providing material to a licensee of the material, utilizing aspects of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

As used herein: the terms "audio-visual content" or "A/V content" includes audio, visual and other multimedia content including motion pictures, music, the spoken word, photos, and printed text; "material" and "content" may be used interchangeably, and includes A/V and other distributed content such as computer programs or software; and "proprietary material" means material protected by contract or intellectual property law.

FIG. 1 illustrates, as an example, a flow diagram of a method for securely providing material to a licensee of

the material that may be performed by one or more servers. In **101**, a content or material request is received from a client. The client in this case may be a person, or a client device such as a computer, a set-top box, network appliance, wireless communicating device such as a personal digital assistant ("PDA") or other type of electronic device. Along with the content request that identifies the content being requested such as, for example, a movie or music title, information identifying a client device or its operator may also be provided. In the case of the client device, this may take the form of a host or network interface card identification number, and in the case of the operator, this may take the form of a credit card number or user identification and password. For establishing secure communications between electronic devices, a public key "KU" may also be provided along with the content request. In such case, a conventional authentication and key exchange procedure may be performed to establish a secure channel.

In **102**, the transaction is authorized in a conventional manner. Preferably this takes the common form of verifying that the requester or operator of the client has properly paid for the requested content and is not otherwise prohibited from receiving it. Payment may be by credit card with conventional bank confirmation. In addition, the requester may also be first required to accept terms of a license agreement in a click-the-button or other conventional manner before the transaction is authorized.

In **103**, a license detailing the usage rights purchased by the requester is provided to the client. The usage rights may include many conventional items such as the number of allowed viewings or playing of material such as a movie, music recording, electronic book, entertainment event or software program. They may also include such things as the time period over which such viewings or playing is allowed. U.S. Pat. No. 5,715,403 entitled "System for

Controlling the Distribution and Use of Digital Works having Attached Usage Rights where the Usage Rights are defined by a Usage Rights Grammar", which is incorporated in its entirety herein by this reference, gives numerous examples of such usage rights.

In **104**, at least one license key "KL" corresponding to the license is provided preferably at the same time as the license to the client. As will be discussed in more detail below, a primary purpose of the at least one license key "KL" is to provide a second level of security by encrypting an at least one content key "KC" that is in turn, used to encrypt the requested content prior to its transmission to the client. In one embodiment of the invention, the at least one license key comprises a plurality of license keys that are used one-at-a-time in a predetermined fashion for encrypting the at least one content key.

In **105**, the at least one content key "KC" is conventionally generated. In **106**, the at least one content key is encrypted by the at least one license key in a conventional manner. Where the at least one license key comprises a plurality of license keys for encrypting and decrypting the at least one content key, the plurality of license keys are preferably used one-at-a-time in a predetermined fashion for such encryption and corresponding decryption. For example, they may be used on a periodically rotating time basis for encrypting and decrypting the at least one content key. Thus, with the many possible combinations of license and content keys, increased security is provided using the method.

In **107**, the requested material is encrypted with the at least one content key "KC" in a conventional manner. Where the at least one content key comprises a plurality of content keys for encrypting and decrypting the requested material, the plurality of content keys are preferably used

one-at-a-time in a predetermined fashion for such encryption and corresponding decryption, depending upon the application. In **108**, the content key encrypted with the license key (also referred to herein simply as the "encrypted content key") and the material encrypted with the at least one content key (also referred to herein simply as the "encrypted material" or "encrypted content") are provided to the client, either in separate transactions or in the same transaction. The order of the separate transactions is generally not important. The encrypted material may be provided as a file or streaming media.

In one application example where the requested content or material is included in at least one MPEG-4 bit stream such as its video and audio bit streams, the at least one content key conventionally comprises a plurality of content keys that are used one-at-a-time in a predetermined fashion for encrypting corresponding time periods of the material. Alternatively, they may be used one-at-a-time in a predetermined fashion for encrypting corresponding portions of the material. The at least one content key in this case is encrypted with the at least one license key, and included in an IPMP ("Intellectual Property Management & Protection") stream that is provided to the licensee along with the material included in the MPEG-4 bit stream that is encrypted with the at least one content key. The at least one content key in this case is conventionally mapped to corresponding portions of the material included in the at least one MPEG-4 bit stream that is encrypted with the at least one content key, by IPMP descriptors associated with the corresponding portions.

FIG. 2 illustrates, as an example, a flow diagram of a method for securely providing material to a licensee of the material that may be performed by a client and is complementary to the method described in reference to **FIG. 1**. In **201**, a content or material request is made by a

client. The client in this case may be a person, or a client device such as a computer, a set-top box, network appliance, wireless communicating device such as a PDA or other type of electronic device. Along with the content request that identifies the content being requested such as, for example, a movie or music title, information identifying a client device or its operator may also be provided. In the case of the client device, this may take the form of a host or network interface card identification number, and in the case of the operator, this may take the form of a credit card number or user identification and password. For establishing secure communications between electronic devices, a public key "KU" may also be provided along with the content request. In such case, a conventional authentication and key exchange procedure may be performed to establish a secure channel, thus providing a third level of security through three key levels (i.e., KU, KL and KC).

In **202**, a license detailing the usage rights purchased by the requester is received. In **203**, at least one license key "KL" corresponding to the license is also received, either along with the license or in a separate transaction. In **204**, the requested material is received encrypted with at least one content key. In **205**, the at least one content key "KC" is received encrypted with the at least one license key, either along with the encrypted material or in a separate transaction. When the encrypted material and the encrypted at least one content key are received in separate transactions, the order that they are received is generally not important. When the encrypted at least one content key is provided with the encrypted material, such as in the case of the MPEG-4 example described above, the encrypted at least one content is extracted from the combination.

In **206**, the encrypted at least one content key is decrypted using the at least one license key in a

conventional manner. Where the at least one content key comprises a plurality of content keys, and/or the at least one license key comprises a plurality of license keys, such decryption generally follows a complementary process to the encryption described in reference to **106** of **FIG. 1**. In **207**, the encrypted content or material is then decrypted using the at least one content key in a conventional manner. Where the at least one content key comprises a plurality of content keys, such decryption generally follows a complementary process to the encryption described in reference to **107** in **FIG. 1**. In **208**, the content is then used in accordance with the license, using conventional control software installed on the client device. The at least one license key in such case may also be used in certain applications to effectively activate the license so that it may be used with the control software.**FIGS. 3~4** illustrate, as examples, block diagrams of representative systems for securely providing material to a licensee of the material. In **FIG. 3**, a server **301** performs the method described in reference to **FIG. 1**, and a client **302** performs the method described in reference to **FIG. 2**. In this case, all transmissions between the server **301** and the client **302** go through a communication medium **303**, which may be, for examples, the Internet or a direct connection through cable, satellite, digital subscriber line ("DSL") or other telephone modem.

In **FIG. 4**, a server **401** likewise performs the method described in reference to **FIG. 1**, and a client **402** likewise performs the method described in reference to **FIG. 2**. In this case, however, certain portions of the methods described in reference to **FIGS. 1** and **2**, such as, for example, the content request and transmission of the encrypted content and encrypted at least one content key, go through a communication medium **403**, and other portions of the methods described in reference to **FIGS. 1** and **2**, such

as, for example, the transmission of the license and the license key, go through another communication medium **404** for additional security.

In **FIG. 5**, servers **501** and **503** combine to perform the method described in reference to **FIG. 1**, whereas client **502** performs the method described in reference to **FIG. 2**. In this system, the server **501** is referred to as a content or data providing server, because it preferably performs portions of the method described in reference to **101**, **102** and **105~108** in **FIG. 1**. The server **503**, on the other hand, is referred to as a license server, because it preferably performs the remaining portions of the method described in reference to **103** and **104** in **FIG. 1**. Other arrangements of multi-server systems are also fully contemplated to be within the full scope of the present invention. U.S. Pat. No. 6,202,056 B1 entitled "Method for Computer Network Operation Providing Basis for Usage Fees", which is incorporated in its entirety herein by this reference, is just one example of a multi-server system in which the present invention may be employed.

Although the various aspects of the invention have been described with respect to preferred embodiments, it will be understood that the invention is entitled to full protection within the full scope of the appended claims.

CLAIMS

I claim:

1. A method for securely providing material to a licensee of the material, comprising:

providing at least one license key to a licensee of material;

providing said material encrypted with at least one content key to said licensee; and

providing said at least one content key encrypted with said at least one license key to said licensee.

2. The method according to claim 1, further comprising providing a license authorizing said licensee to use said material.

3. The method according to claim 2, wherein said license includes a plurality of usage rights for using said material.

4. The method according to claim 2, wherein said at least one license key is provided along with said license to said licensee.

5. The method according to claim 1, wherein said providing at least one license key to a licensee of material, comprises providing said at least one license key encrypted with a public key of said licensee to said licensee.

6. The method according to claim 1, wherein said at least one license key and said material encrypted with said at least one content key are provided by transmitting them through different communication mediums to said licensee.

7. The method according to claim 1, wherein said at least one content key encrypted with said at least one license key is provided to said licensee along with said material encrypted with said at least one content key.

8. The method according to claim 7, wherein said at least one content key encrypted with said at least one license key and said material encrypted with said at least one content key are provided by transmitting them over an authenticated secure channel to said licensee.

9. The method according to claim 1, wherein said providing said material encrypted with at least one content key to said licensee, comprises encrypting said material in real-time with said at least one content key and providing said material encrypted with said at least one content key to said licensee by transmitting it as streaming media.

10. The method according to claim 1, wherein said material is included in at least one MPEG-4 bit stream encrypted with said at least one content key.

11. The method according to claim 10, wherein said at least one content key encrypted with said at least one license key is included in an IPMP stream provided to said licensee along with said material included in said at

least one MPEG-4 bit stream encrypted with said at least one content key.

12. The method according to claim 11, wherein said at least one content key encrypted with said at least one license key is mapped to corresponding portions of said material included in said at least one MPEG-4 bit stream encrypted with said at least one content key, by IPMP descriptors associated with said corresponding portions.

13. The method according to claim 11, wherein said at least one content key includes a plurality of content keys for encrypting and decrypting corresponding portions of said material.

14. The method according to claim 11, wherein said at least one content key includes a plurality of content keys for encrypting and decrypting corresponding time periods of said material.

15. The method according to claim 14, wherein said plurality of content keys are used one-at-a-time in a predetermined fashion for encrypting and decrypting said corresponding time periods of said material.

16. The method according to claim 11, wherein said at least one license key includes a plurality of license keys for encrypting and decrypting said at least one content key.

17. The method according to claim 16, wherein said plurality of license keys are used one-at-a-time in a

predetermined fashion for encrypting and decrypting said at least one content key.

18. An apparatus for securely providing material to a licensee of the material, comprising at least one server configured to:

transmit at least one license key to a client device operable by a licensee of material;

transmit said material encrypted with at least one content key to said client device; and

transmit said at least one content key encrypted with said at least one license key to said client device.

19. The apparatus according to claim 18, wherein said at least one server is further configured to transmit a license authorizing said licensee to use said material.

20. The apparatus according to claim 19, wherein said license includes a plurality of usage rights for using said material.

21. The apparatus according to claim 19, wherein said at least one server is further configured to establish an authenticated secure channel with said client device and transmit said at least one license key along with said license to said client device over said secure channel.

22. The apparatus according to claim 18, wherein said at least one server comprises a license server configured to transmit said at least one license key to said client device, and a data providing server configured to transmit said material encrypted with at least one content

key and said at least one content key encrypted with said license key, to said client device.

23. The apparatus according to claim 18, wherein said material is included in at least one MPEG-4 stream encrypted with said at least one content key.

24. The apparatus according to claim 23, wherein said at least one content key encrypted with said at least one license key is included in an IPMP stream provided to said licensee along with said material included in said at least one MPEG-4 bit stream encrypted with said at least one content key.

25. The apparatus according to claim 24, wherein said at least one content key encrypted with said at least one license key is mapped to corresponding portions of said material included in said at least one MPEG-4 bit stream encrypted with said at least one content key, by IPMP descriptors associated with said corresponding portions.

26. The apparatus according to claim 23, wherein said at least one content key includes a plurality of content keys for encrypting and decrypting corresponding portions of said material.

27. The apparatus according to claim 23, wherein said at least one content key includes a plurality of content keys for encrypting and decrypting corresponding time periods of said material.

28. The apparatus according to claim 27, wherein said plurality of content keys are used one-at-a-time in a predetermined fashion for encrypting and decrypting said corresponding time periods of said material.

29. The apparatus according to claim 24, wherein said at least one license key includes a plurality of license keys for encrypting and decrypting said at least one content key.

30. The apparatus according to claim 29, wherein said plurality of license keys are used one-at-a-time in a predetermined fashion for encrypting and decrypting said at least one content key.

31. A system for securely providing material to a licensee of the material, comprising:

a client device operable by a licensee of material; and

at least one server configured to transmit at least one license key, said material encrypted with at least one content key, and said at least one content key encrypted with said at least one license key to said client device.

32. The system according to claim 31, wherein said at least one server is further configured to transmit a license authorizing said licensee to use said material to said client device.

33. The system according to claim 32, wherein said license includes a plurality of usage rights for using said material.

34. The system according to claim 32, wherein said at least one server is further configured to establish an authenticated secure channel with said client device and transmit said at least one license key along with said license to said client device over said secure channel.

35. The system according to claim 31, wherein said at least one server comprises a license server configured to transmit said at least one license key to said client device, and a data providing server configured to transmit said encrypted material and said encrypted at least one content key to said client device.

36. The system according to claim 31, wherein said material is included in at least one MPEG-4 stream encrypted with said at least one content key.

37. The system according to claim 36, wherein said at least one content key encrypted with said at least one license key is included in an IPMP stream provided to said licensee along with said material included in said at least one MPEG-4 bit stream encrypted with said at least one content key.

38. The system according to claim 37, wherein said at least one content key encrypted with said at least one license key is mapped to corresponding portions of said material included in said at least one MPEG-4 bit stream encrypted with said at least one content key, by IPMP descriptors associated with said corresponding portions.

39. The system according to claim 36, wherein said at least one content key includes a plurality of content keys for encrypting and decrypting corresponding portions of said material.

40. The system according to claim 36, wherein said at least one content key includes a plurality of content keys for encrypting and decrypting corresponding time periods of said material.

41. The system according to claim 40, wherein said plurality of content keys are used one-at-a-time in a predetermined fashion for encrypting and decrypting said corresponding time periods of said material.

42. The system according to claim 37, wherein said at least one license key includes a plurality of license keys for encrypting and decrypting said at least one content key.

43. The system according to claim 42, wherein said plurality of license keys are used one-at-a-time in a predetermined fashion for encrypting and decrypting said at least one content key.

44. The system according to claim 31, wherein said client device is configured to:

decrypt said encrypted at least one content key using said license key; and

decrypt said encrypted material using said decrypted at least one content key.

45. The system according to claim 44, wherein said client device is further configured to receive said license key along with a license authorizing said licensee to use said material from said at least one server.

46. The system according to claim 45, wherein said license includes a plurality of usage rights for using said material.

47. The system according to claim 46, wherein said client device is further configured to use said material only in accordance with said plurality of usage rights of said license.

48. A method for securely providing material to a licensee of the material, comprising:

providing a license to use material and a license key corresponding to said license;

providing said material encrypted with a content key; and

providing said content key encrypted with said license key.

49. The method according to claim 48, wherein said license includes a plurality of usage rights for using said material.

50. The method according to claim 48, wherein said encrypted content key is provided with said encrypted material.

51. The method according to claim 48, wherein said license, said license key, said encrypted material, and said encrypted content key are provided by electronically transmitting them to a client requesting said material.

52. A method for securely providing material to a licensee of the material, comprising:

receiving a license to use material and a license key corresponding to said license;

receiving said material encrypted with a content key;

receiving said content key encrypted with said license key;

decrypting said encrypted content key using said license key; and

decrypting said encrypted material using said decrypted content key.

53. The method according to claim 52, wherein said license includes a plurality of usage rights for using said material.

54. The method according to claim 52, wherein said encrypted content key is received with said encrypted material.

55. The method according to claim 52, wherein said license, said license key, said encrypted material, and said encrypted content key are received electronically.

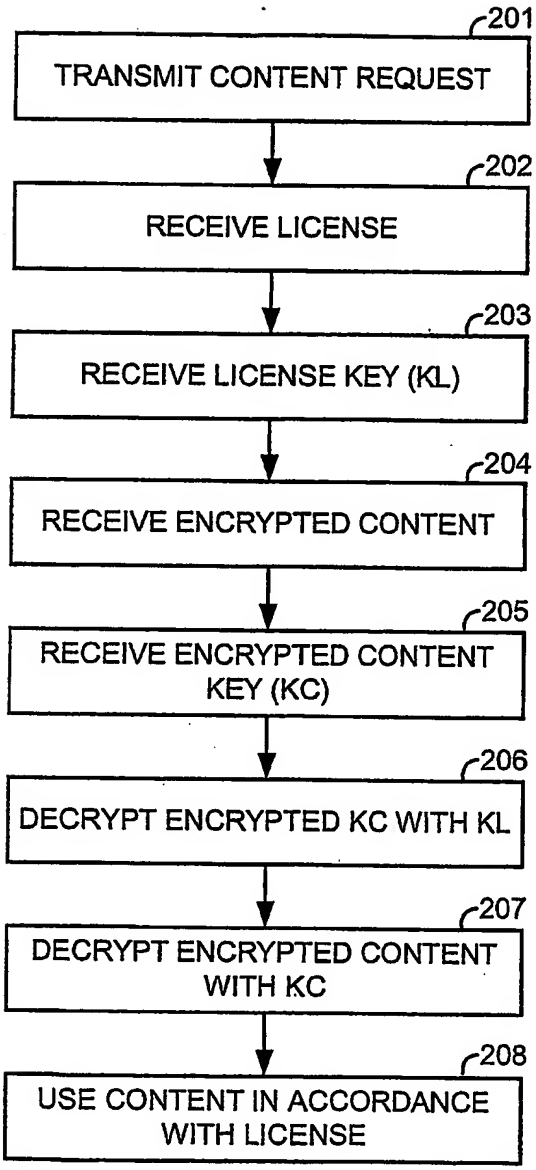
201
TRANSMIT CONTENT REQUEST
202
RECEIVE LICENSE
203
RECEIVE LICENSE KEY (KL)
204
RECEIVE ENCRYPTED CONTENT
205
RECEIVE ENCRYPTED CONTENT KEY (KC)
206
DECRYPT ENCRYPTED KC WITH KL
207
DECRYPT ENCRYPTED CONTENT WITH KC
208
USE CONTENT IN ACCORDANCE WITH LICENSE

FIG.2

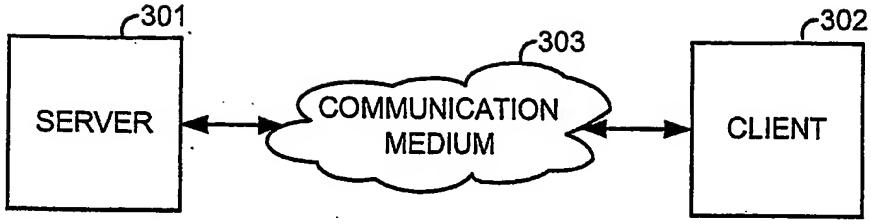

FIG.3

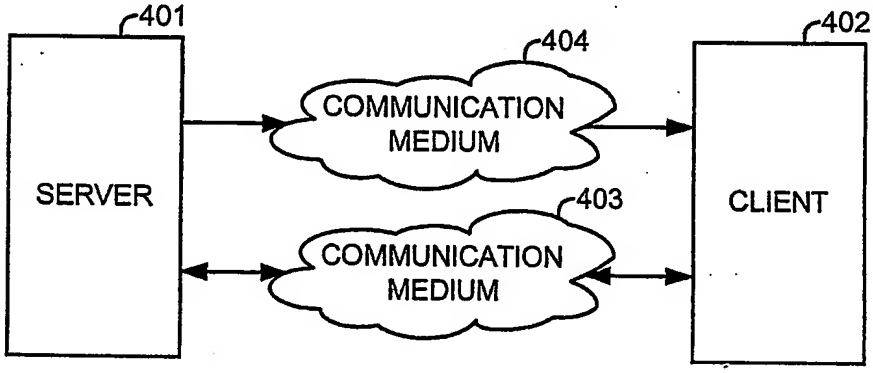

FIG.4

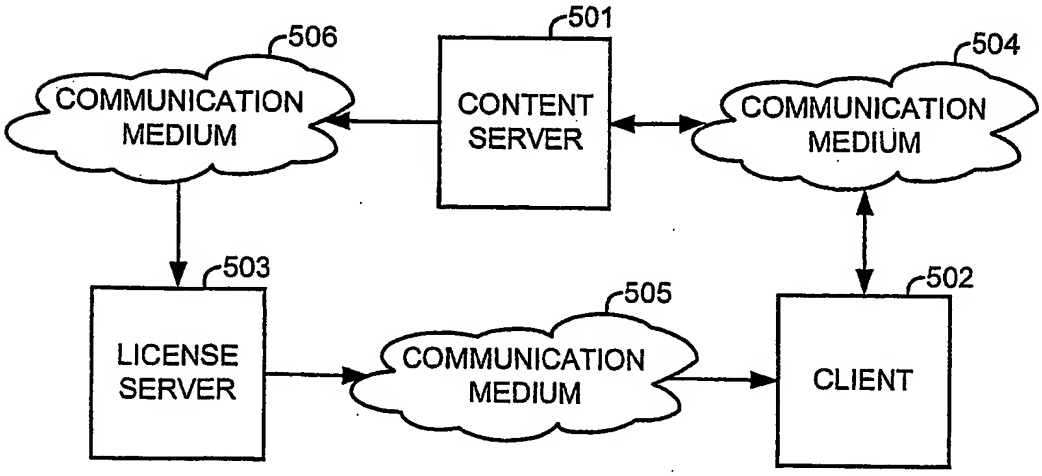

FIG.5